If you have questions or comments, please contact:

Tony Campbell
Enterprise IT Security Specialist
tcampbell@rochestermn.gov
(507) 328-2848

Section 6: Access Control

Section 6: Access Control

Access controls are security features that govern how users and processes communicate and interact with systems and resources. The objective of implementing access controls is to ensure that authorized users and processes are able to access information and resources while preventing unauthorized users and processes access.

Goals of Section 6: Access Control

- To require that the person or system seeking access to secured information, information systems, or devices be positively identified.
- To ensure that only authorized users and processes gain access, and only the minimum access required to perform a given role effectively.
- To logically group network assets, resources, and applications for the purpose of auditing and applying security controls.
- Define the requirements for secure design, configuration, management, administration, and oversight of border devices.
- Assign responsibility and set the requirements for remote access connections to the internal network.
- Assign responsibility and set the requirements for teleworking.
- To ensure that there is a means to prevent and/or detect attempts to gain access to information resources by unauthorized entities.

Access Control Policy Index

6.7. User Access Control and Authorization

6.8. Administrative and Privileged Accounts

6.9. Monitoring System Access and Use

6.0 Access Control Policy

6.1. Authentication Policy

6.1.1. Access to and use of information technology systems should require an individual to uniquely identify and authenticate him/herself to the resource.

6.1.2. Multi-user or shared accounts require a documented and justified reason. Shared accounts are at the discretion of the IT Leadership Team. Shared accounts must follow the exception process outlined in the Governance and Risk Management policy. The Enterprise IT Security Specialist must inform the Technology Steering Committee of shared accounts at least annually.

6.1.3. The Enterprise IT Security Specialist is responsible for managing an annual user account audit of network accounts, local application accounts, and web application accounts. The audit results must be reported to the Technology Steering Committee.

6.1.4. Data classification, regulatory requirements, the impact of unauthorized access, and the likelihood of a threat are all risk assessment factors in considering the appropriate level of authentication required. The IT Leadership Team will use this assessment to determine the appropriate controls and recommend for approval by the Technology Steering Committee.

6.1.5. Access to systems, applications, or data that is not public requires multi-factor authentication or enhanced single factor authentication as identified in the password standard.

6.1.5.1. Password complexity documentation is in the City Password Standard.

6.1.5.2. The Acceptable Use Policy will contain the City Password Standard.

6.1.5.3. The inability to enforce this standard through technical means does not negate the requirement. Systems that are incapable of complying require a documented exception (see Section 1 Governance policy). Exceptions will be reported to the Technology Steering Committee at least annually.

6.1.66.1.6. Where multi-factor authentication is not available, passwords and PINs must be unique to the application.

. 6.1.7. In the event of a suspected or confirmed compromise in an authentication mechanism, the user must immediately contact the City, Library, or RPU help desk.

6.2. Access Control Authorization

6.2.1. Default access privileges will be set to “deny”

6.2.2. Access to information and information systems for personnel and processes requires that the access is essential to fulfill their duties per 13.05 of MN Government Data Practices Act.

6.2.3. Access permissions will be the minimum required to perform a job or program function.

6.2.4. Information and information system owners are responsible for determining access rights and permissions. The IT Leadership team will review permission requests for appropriate application of the principle of least privilege.

6.3. Network Segmentation

6.3.1. The segregation of the network infrastructure into distinct segments is required. Segmentation should be based upon data classification, department, physical location, and asset type (servers, DMZ servers, printers, etc.). Segmentation should assist in controlling the flow of data to less trusted segments, access based on need to know, defining the network for monitoring purposes, and limiting an attacker’s ability to pivot the network.

6.3.2. Complete documentation of the network topology and architecture including an up-to-date network diagram showing all internal (wired and wireless) connections, external connections, endpoint groups (PC’s Smartphones, etc), including the Internet is required. The diagram should clearly identify the key infrastructure, monitoring and security zone segmentation scheme.

6.3.2.1 Network documentation must be updated whenever there is a change to the network topology or architecture.

6.4. Border Device Security

6.4.1. Border security devices require secure implementation and maintenance to restrict access between networks that are trusted to varying degrees.

6.4.2. If any situation renders the Internet-facing border security devices inoperable, disabling Internet service is required unless mitigating controls can be put in place.

6.4.3. IT Managers are responsible for maintaining, and managing border security devices in their locations.

6.4.4. The default policy for handling inbound and outbound traffic should be to deny all.

6.4.4.1. Types of network traffic the City allows requires documentation in the Border Security Standards.

6.4.4.2. Rule-sets must be as specific and simple as possible. Rule-set documentation will include the business justification for allowed traffic.

6.4.4.3. All configuration and rule-set changes are subject to a risk assessment and the City change management process.

6.4.5. All border security devices must be physically located in a controlled environment, with access limited to authorized personnel only.

6.4.6 DMZ, or internet connections must be physically and logically separate from internal systems, storage, or internal virtual systems.

6.4.6. To support recovery after failure or natural disaster, the border security device's configuration, policy, and rules require backup or replication at least annually as well as before and after every configuration change including software or firmware updates.

6.4.7. Border devices must log successful and failed activity as well as configuration changes. Failed logon attempts will be reported to IT Leadership Team at least monthly.

6.4.9. Annual configuration and rule-set review of border devices, by the IT Leadership Team, is required.

6.4.9.1. All External interfaces and a representative sample of the internal network will be tested by a qualified independent entity at least annually.

6.4.9.2. Submission of review results to the Technology Steering Committee is required at least annually.

6.5. Remote Access

6.5.1. The IT Leadership Team is responsible for approving remote access connections and security controls.

6.5.2. Multifactor authentication is required for remote access.

6.5.2.1. One of the multi-factors shall be "out-of-band."

6.5.3. Remote equipment must be configured in accordance with City workstation, or mobile device, security standards.

6.5.4. Business partners and vendors wishing to obtain approval for remote access to computing resources must have access approved by the IT Leadership Team. The partner or vendor must provide documentation supporting that their employee has undergone a background check. Their City sponsor is required to provide a valid business reason for remote access.

6.5.5. Employees, business partners, and vendors approved for remote access must sign a Remote Access Agreement that acknowledges their responsibilities prior to gaining access. Access and accounts should automatically disable after 90 days. A member of the IT Leadership Team may authorize

reinstating access. The full agreement, including supporting background check documentation, must be renewed annually.

6.5.6 The Enterprise IT Security Specialist will provide report at least annually to the Technology Steering Committee, of third-parties having remote access as well as third-parties that are provided confidential information. The report must include an assessment of the third-parties' security measures.

6.6. Teleworking Policy

6.6.1. Teleworking schedule requests require written submission by management and authorization by the Office of Human Resources.

6.6.2. The Office of Human Resources is responsible for notifying the IT Leadership Team of both approved and denied teleworking privileges.

6.6.3. Teleworking equipment including connectivity devices must be configured in accordance with City security standards.

6.6.4. IT Managers, or their designees, are responsible for managing, maintaining, and monitoring the configuration of and the connection to the teleworking location.

6.6.5. Remote access is in accordance with the Remote Access policy and standards.

6.6.6. The teleworker is responsible for the physical security of the telecommuting devices.

6.6.8. Monitoring the teleworker's performance is the responsibility of their immediate supervisor.

6.7. User Access Control and Authorization

6.7.1. Default user access permissions will be set to "deny" prior to the determination of specific permissions based on role and/or job function.

6.7.2. Access to City information and systems is only required for workforce personnel with a need-to-know to perform their job function(s).

6.7.3. Access shall be restricted to the minimal amount required to carry out the business requirement of the access.

6.7.5. Information owners are responsible for annually reviewing and authorizing user access permissions to data classified as "medium" or "high risk".

6.8. Administrative and Privileged Accounts

6.8.1. Request for assignment of administrator-level accounts or changes to privileged group membership require approval by the IT Leadership Team.

6.8.2. Administrative and privileged user accounts usage is only for performing duties requiring administrative or privileged access.

6.8.3. All administrative and privileged account holders will have a second user account for performing any function where administrative or privileged access is not required.

6.8.4. Activation of user accounts assigned to contractors, consultants, or service providers requiring administrative or privileged access must be approved by the IT Leadership Team.

6.8.5 The Enterprise IT Security Specialist will inform the Technology Steering Committee of third-party administrative accounts at least annually.

6.8.6. Administrative and privileged account requires dual factor authentication and activity must be logged.

6.9. Monitoring System Access and Use

6.9.1. The IT Leadership Team is responsible for determining the extent of logging and analysis required for information systems storing, processing, transmitting, or providing access to information classified as “high risk” or “medium risk”.” However, at a minimum, logging must include the following:

6.9.1.1. Both successful and failed network authentication attempts.

6.9.1.2. Both successful and failed authentication attempts to any application that stores or processes information classified as “high risk”.

6.9.1.3. Any action, or attempted failed action, by an administrator or other privileged account to the network or to an application.

6.9.1.4. Both successful and failed password change attempts.

6.9.1.5 Successful and failed attempts to access, modify, or destroy “high risk” or “medium risk” data.

6.9.1.6. Log data shall include, at a minimum, date and time of the event, The system component (hardware, software) where the event occurred, the type of event, the user or subject identity, and the outcome (success or failure).